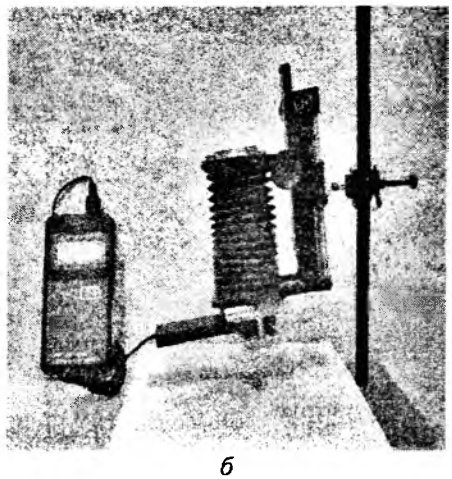

б

Рисунок 2 – Устройство для оценки площади напыленного слоя проявителя: *а* – схема, *б* – фотография

С целью обеспечения возможности оценки площади покрытия изделия слоем проявителя в производственных условиях разработано простое устройство, принцип действия которого основан на использовании естественного дневного освещения. Схема и фотография устройства показана на рисунке 2.

Данное устройство включает штатив 1, на котором закреплена фотографическая насадка 2 с раздвижным мехом (макромех). В нижней части насадки закреплен измерительный датчик 4 люксметра 5. Использование макромеха позволяет существенно снизить погрешность измерений, возникающую за счет рассеивания и отражения светового потока, попадающего на светочувствительный элемент люксметра. Измеряемый образец 3 размещается в верхней части насадки 2. Также как и в установке на рисунке 1, здесь оценка площади напыленного покрытия определяется по показаниям люксметра.

Выводы

Разработаны и изготовлены экспериментальные установки для оценки площади покрытия деталей и изделий слоем проявителя, используемые при капиллярном контроле по новой технологии с неполным по площади нанесением проявителя [2].

Устройства позволяют оперативно определять степень покрытия поверхности образца слоем суспензионных и порошковых проявителей в лабораторных и производственных условиях.

1. Прохоренко, П.П Введение в теорию капиллярного контроля / П.П. Прохоренко, Н.П. Мигун // Мн.: Наука и техника. – 1988. – С. 207.
2. Мигун, Н.П. Капиллярный контроль при тонких слоях проявителя / Н.П. Мигун, Н.В. Деленковский, А.Б. Гнусин // Современные методы и приборы контроля качества и диагностики состояния объектов: материалы 4-ой междунар. науч.-техн. конф. – Могилев – 2012. – С. 77-78.
3. Мигун, Н.П. Компьютеризированная система определяет качество дефектоскопических материалов / Н.П. Мигун, А.Б. Гнусин, И.В. Волович. // Промышленная безопасность. – 2004. – № 1. – С. 34–36.
4. EN ISO 3452-2:2006. Non-destructive testing – Penetrant testing – Part 2: Testing of penetrant materials.
5. СТБ 1172-99. Контроль неразрушающий. Контроль проникающими веществами (капиллярный).

УДК 004.932.72

НЕЙРОНЕЧЁТКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Миков Д.А.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Весьма перспективным подходом к обеспечению информационной безопасности в автоматизированных системах является моделирование, основанное на создании и исследовании моделей, описывающих функционирование этих систем. Применение подобных моделей позволяет проанализировать и оптимизировать процессы сбора, хранения и обработки информации, а также выбрать технологии защиты данных.

Основное преимущество нечётких моделей, по сравнению с традиционными математическими моделями, связано с возможностью использования для их разработки значительно меньших объёмов информации о моделируемой системе. При этом информация может носить приближённый, нечёткий характер, что является особенно эффективным для такого сложного и неоднозначного процесса как обеспечение информационной безопасности в автоматизированных системах [1].

Под нечётким множеством A, определённым на X, понимается совокупность:

$$A=\{(x,\mu_A(x))|x\epsilon X\},$$

где X – область значений, а $\mu_A(x)$ – функция принадлежности, характеризующая степень принад-

лежности элемента x нечёткому множеству A от 0 до 1, т.е. $0 \le \mu_A(x) \le 1$.

Как правило, нечёткие модели разрабатываются для систем нечёткого управления, поэтому типичная структура состоит из 3 блоков:

1) блок фаззификации (занимается вычислением степени принадлежности чётких входных параметров нечётким множествам);

2) блок вывода (набор логических правил, которые задают причинно-следственные связи между входом и выходом);

3) блок дефаззификации (вычисление чёткого выходного значения на основе результирующей функции принадлежности, которая рассчитывается механизмом вывода в блоке вывода).

Идея применения данной концепции к нечёткому управлению динамическими объектами принадлежит Мамдани. Модель Мамдани представляет собой множество правил:

ЕСЛИ (x есть A) ТО (y есть B),

где A, B – нечёткие множества. Каждое правило задаёт в указанном пространстве некоторую нечёткую точку. На основе множества нечётких точек формируется нечёткий график.

Первые нечёткие модели создавались на основе экспертных знаний о моделируемой системе. Получение информации о системе осуществлялось с помощью эксперта в соответствующей предметной области, а затем эксперт в области нечёткого моделирования выполнял преобразование этой информации в нечёткую модель. Указанный метод называется приобретением знаний и является эффективным в том случае, если эксперт полностью обладает знаниями о системе и может выразить эти знания в словесной форме и передать их.

В случае с информационной безопасностью знания эксперта часто являются неполными, неточными, слабо поддающимися формулированию и могут даже содержать в себе противоречия. Кроме того, эти знания субъективны, то есть мнения отдельных людей о функционировании одной и той же информационной системы могут различаться. С учётом всего сказанного, представляется целесообразным, чтобы в основе модели лежала объективная информация о системе. Такой информацией являются результаты измерения значений её входов и выходов.

Процесс приобретения знаний на основе этих данных называется извлечением знаний. Такой возможностью обладают нейронные сети [2]. Целесообразно объединить возможности нечётких моделей и нейросетевых методов.

Нейронечёткая сеть представляет собой особую эквивалентную форму нечёткой модели. Растущий интерес к нейронечётким сетям (ННС) обусловлен следующими их неоспоримыми преимуществами по сравнению с обычными нечёткими моделями:

1) ННС обеспечивают возможность оптимизации (настройки) параметров нечётких моделей на основе данных измерения входов и выходов реальных систем;

2) ННС позволяют корректировать недостаточно точные нечёткие модели, формируемые экспертами;

3) ННС дают возможность расширения формируемых экспертами нечётких моделей на те области пространства входов, экспертные знания о которых отсутствуют.

Методика преобразования нечёткой модели в нейронечёткую сеть является достаточно сложной и зависит от типа модели.

Чтобы использовать нейронечёткую сеть для обеспечения информационной безопасности, необходимо определить, какие данные должны быть на входе и выходе системы. Наиболее наглядный пример - оценка информационных рисков на выходе нейронечёткой сети, с помощью которой можно сделать вывод об уровне защищённости информации.

Из определения риска информационной безопасности следует, что величина риска R есть функция от потенциально возможного ущерба A, угрозы информационной безопасности T и уязвимости информационной системы V:

$$R=f(A,T,V).$$

Входными факторами будут экспертные оценки угрозы, ущерба и уязвимости, описанных лингвистическим множеством {очень низкий, низкий, средний, высокий, очень высокий}.

Также следует использовать данные системы обнаружения вторжений, антивирусов, межсетевых экранов о потенциально опасной активности, общем уровне сетевой активности и нагрузки на тот или иной участок системы.

Шкала угроз включает уровни:

1) очень низкий – событие практически никогда не происходит;

2) низкий – событие случается редко;

3) средний – событие вполне возможно при определённом стечении обстоятельств;

4) высокий – скорее всего, событие произойдёт при организации атаки;

5) очень высокий – событие, вероятнее всего, произойдёт при организации атаки.

Шкала ущерба содержит уровни:

1) очень низкий – приводит к незначительным потерям материальных средств и ресурсов, которые быстро восполняются, или к незначительному влиянию на репутацию;

2) низкий – приводит к более заметным потерям материальных активов, более существенному влиянию на репутацию или ущемлению интересов;

3) средний – приводит к достаточным потерям материальных активов или ресурсов или наносится достаточный урон репутации и интересам;

4) высокий – наносится значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности;

5) очень высокий – приводит к разрушительным последствиям и невозможности ведения деятельности.

Шкала уязвимостей состоит из уровней:

1) очень низкий – уязвимость, которой можно пренебречь;

2) низкий – незначительная уязвимость, которую легко устранить;

3) средний – умеренная уязвимость;

4) высокий – серьёзная уязвимость, ликвидация которой возможна, но связана со значительными затратами;

5) очень высокий – критическая уязвимость, которая ставит под сомнение возможность её устранения.

В итоге на выходе системы будет получена оценка уровня риска информационной безопасности на основе входных данных, описанная расширенным лингвистическим множеством {пренебрежимо низкий, очень низкий, низкий, ниже среднего, умеренный, выше среднего, высокий, очень высокий, критический}.

Шкала уровней рисков выглядит так:

1) пренебрежимо низкий – риском можно пренебречь;

2) очень низкий – если сведения расцениваются как очень низкий риск, необходимо определить, существует ли необходимость в корректирующих действиях, или есть возможность принять этот риск;

3) низкий – уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы;

4) ниже среднего – необходимо разработать и применить план корректирующих действий в течение приемлемого периода времени;

5) умеренный – уровень риска не позволяет стабильно работать, имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы в сторону уменьшения риска;

6) выше среднего – система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее;

7) высокий – уровень риска такой, что бизнес-процессы находятся в неустойчивом состоянии;

8) очень высокий – необходимо незамедлительно принять меры по уменьшению риска;

9) критический – уровень риска очень большой и является недопустимым для организации, что требует прекращения эксплуатации системы и принятия радикальных мер по уменьшению риска.

При реализации представленной методики оценки информационных рисков для ввода исходных данных и интерпретации результатов целесообразно воспользоваться пакетом Fuzzy Logic Toolbox системы MATLAB.

1. Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков // Вестник МГТУ. Серия «Приборостроение». Специальный выпуск СВ-5 «Информатика и системы управления». – 2012. - С 261-271.
2. Булдакова Т.И., Суятинов С.И. Нейрокомпьютерные системы. – Саратов: Изд. СГТУ. - 1999. - 92с.

УДК 614.842

ОСОБЕННОСТИ ОПРЕДЕЛЕНИЯ СООТВЕТСТВИЯ ПРИБОРОВ И ОБОРУДОВАНИЯ КАТЕГОРИЯМ ОПАСНОСТИ ПОМЕЩЕНИЙ

Мисюкевич Н.С.
Белорусский национальный технический университет
Минск, Республика Беларусь

Категории производственных и складских помещений и зданий (Ф5.1, Ф5.2, Ф5.3 согласно [1]) и наружных установок по взрывопожарной и пожарной опасности определяются расчетом по [2]. Приборы и оборудование, применяемые в технологическом процессе, должны соответствовать по безопасности категории и группе смеси, которая может находиться и (или) образовываться в объеме помещений как в условиях нормальной эксплуатации, так и при аварии. При определении параметров соответствия можно или подбирать соответствующее оборудование, или уменьшать опасность среды, в котором оно применяется. В каждом конкретном случае решение целесообразно принимать исходя из экономических показателей.

При определении показателей среды допускается использование справочных данных, опубликованных в официальных изданиях [2]. Возможно упрощение расчетов по ряду веществ и материалов с использованием данных ТКП 130-2008 [3]. В работе рассмотрены возможности упрощения методик определения категорий с соблюдением требуемого уровня безопасности [4].

За критерий безопасности для взрывопожароопасных объектов принимается избыточное давление взрыва ΔР, кПа, не превышающее 5 кПа.